PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-196083
(43)Date of publication of application : 21.07.1999

(51)Int.Cl. H04L 9/08
H04L 9/32

(21)Application number : 10-293845
(22)Date of filing : 15.10.1998

(71)Applicant : THOMSON MULTIMEDIA SA
(72)Inventor : CAMPINOS ARNALDO
FISCHER JEAN-BERNARD

(30)Priority
Priority number : 97 9713022 Priority date : 17.10.1997 Priority country : FR

(54) METHOD FOR TRANSFERRING SCRAMBLE KEY

(57)Abstract:
PROBLEM TO BE SOLVED: To obtain the method for transferring a scramble key from a security element to a decoder.
SOLUTION: This transfer method is conducted in an input stage, a challenge stage and an opening stage. In the input stage, a security element, including a scramble key whose cipher, is decoded exchanges a message with a decoder, and as a result, the decoder has items consisting of data representing all or a part of the scramble key whose cipher is decoded and data representing data, capable of authenticating a smart card in a one-to-one form at the end of the input stage. In the challenge state, the data are transferred from the decoder to the smart card. As a result, which of the received data is disclosed is represented. Preferably, explicitness of the received data is conducted at random. In the opening stage, the smart card transfers data of all or a part of the scramble key the cipher of which is decoded to the decoder, together with the data capable of authenticating the smart card.

LEGAL STATUS
[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1] In the approach of transmitting the scramble key decrypted from the security element (1) to the decoder (2) Data of the n beginnings outputted from the security element (1) (X1, Y) () (X2, Y), ..., (Xn, Y) are put in into a decoder (2) (M1, M2, and ...) It is Mj, ..., Mn phase and said n is two or more integers. The phase where each data into which it was put by said n beginnings consists of the first data (Xj) which make all or part (Y), and security element (1) of a scramble key (KD) which were decrypted attest, The 2nd n data (Z1, Y) ((Z2, Y), ... (it Zj(s))) (Zn, Y) to Y), ..., p data (Za1, Y) () (Za2, Y), ..., the data (d) that make it possible to choose (Zap, Y) are the phases of the challenge (C) transmitted to a security element (1) from a decoder (2). Said p is an integer smaller than n. Said each 2nd n data The phase which consists of the 2nd data (Xj) to which authentication of all of the decrypted scramble keys or a part (Y), and a security element (1) is carried out, The phase of opening (O1, O2, ..., Op) which consists of p data transfers chosen from the security element (1) as the decoder (2) in the challenge phase (C), the data (X1, Y) ((X2, Y), and ...) put into the n beginnings p data (O1 (Za1, Y) --) transmitted in p data and the opening phase which were chosen from (Xn, Y) The approach characterized by consisting of a count phase which makes it possible to extract all or the part (Y) of a scramble key decrypted from O2 (Za2, Y), ..., Op (Zap, Y).

[Claim 2] The approach according to claim 1 of consisting of a phase which reconstructs a perfect scramble key when said phase to put in, an opening phase, and a count phase relate to a part of perfect scramble key (KD) (Y) behind said count

phase.
[Claim 3] Said phase (M1, M2, ..., Mj, ..., Mn) to put in is the approach according to claim 1 or 2 consist of three steps (M1, M2, M3), and an opening step (O1, O2, ..., Op) consists of two steps.
[Claim 4] It is [claim 1 performed at random thru/or] an approach given in any 1 term among 3 to choose p data (Za1, Y) ((Za2, Y), ..., (Zap, Y)) from the 2nd n data (Z1, Y) ((Z2, Y), ..., (Zj, Y), ..., (Zn, Y)).
[Claim 5] The data into which it was put by the n beginnings respectively (Cj) It is as a result of the first exclusive-OR function (5) in which the first data (Bj) and 2nd data (Gj) are applied. Said first data (Bj) It is the pseudo-random WORD generated with the application of seed (Sj) in the first pseudo-random generation vessel (4). Said 2nd data (Gj) It is the WORD generated from relating all or the parts of the 3rd data and the decrypted scramble keys (Y). Said opening phase consists of transmitting seed (Sj) and the 2nd data (Gj) to a decoder (2) from a security element (1). Said count phase In order to calculate the 4th data (Ej) based on applying Seed Sj to the 2nd pseudo-random generation machine (8) and to calculate the 5th data (Fj) The 4th data (Ej) and data (Cj) into which it was put are applied to the 2nd exclusive-OR function (9). If the 5th data (Fj) is the same as the 2nd data (Gj) transmitted by opening operation as compared with the 2nd data (Gj) to which the 5th data (Fj) is transmitted by opening operation as a result of a comparison It is [claim 1 which consists of storing decrypted all or the part (Y) of scramble keys thru/or] an approach given in any 1 term among 4.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] the approach this invention transmits a scramble key -- being related -- especially -- conditional -- it is related with the approach of transmitting a scramble key between the security element of an access system, and a decoder. conditional -- only the user who acquired the access which receives the service for its service can be provided with a service provider by the access system. There are for example, charged television systems in such a system.
[0002]
[Description of the Prior Art] The service offered by the service provider consists of an item to which the scramble was able to be applied by the scramble key so that it may be well-known to this contractor. The item to which the scramble was able to be applied is the level of the access assigned to the user, has a scramble canceled and

is read by the user. The following [the scrambled item] IE (ECG) is written. ECG expresses the item which is not scrambled (ECG is the abbreviation for "Electronically Coded Goods").

[0003] In order to carry out scramble discharge of the item, a service provider supplies the scramble key used in order to scramble an item to each user. In order to maintain a scramble key at secrecy, a scramble key is supplied after being enciphered with the algorithm which used Key K. The scramble key as which versatility was enciphered is sent to various users in a control message. Hereafter, ECM [a control message] is written (ECM is the abbreviation for "Entitlement Control Message").

[0004] In order to give access to service only to the user who was able to grant access, a service provider provides each user with a smart card and a decoder. ECM is received by the decoder and a decoder transmits them to a smart card. A smart card contains the key K of the encryption algorithm of a scramble key. A scramble key is decoded by the smart card, it is restored by the decoder, and a decoder can carry out scramble discharge of the received item which was scrambled.

[0005]

[Problem(s) to be Solved by the Invention] The hacker who does the monitor of between a smart card and decoders is in the location which monitors the decrypted scramble key which flows from a smart card to a decoder. This expresses a fault. conditional -- an access system is a stand-alone type system, and since the items IE (ECG) and ECM scrambled in that system are included on the information carrier of a stand-alone like a digital videodisc, this fault is still more serious. It is because the hacker who monitors the scramble key which is not enciphered can store these keys and they of the user who has not obtained authorization can be redistributed unjustly. The scrambled item which is included on a stand-alone information carrier will already be protected.

[0006] conditional -- when an access system is an online type, the scrambled item IE (ECG) is an item which consists of signals to which the space or cable top was simultaneously distributed from the single source to the various customers of a service provider. The hack (disturbance) of the decoded scramble key must be carried out on real time. The conditions of hacking become more difficult. However, there is danger of hacking on a link short enough comparatively until now [high].

[0007] This invention does not have these faults.

[0008]

[Means for Solving the Problem] This invention relates to the approach of transmitting the scramble key decrypted from the security element to the decoder. The above-mentioned approach of carrying out a transfer consists of the next phase. - In a decoder, it is the phase of putting in n data output of the beginning from a security element (pledge), and, as for n, each n data of two or more integers and the beginning into which it was put consists of the first data to which authentication of all of the decrypted scramble keys or a part, and a security element is carried out.

[0009] – One data which makes it possible to choose p data from the 2nd n data is the phase of the challenge transmitted to a security element from a decoder, p is an integer smaller than n and each 2nd n data consists of all of the decrypted scramble keys or parts, and the 2nd data to which authentication of a security element is carried out.
[0010] – The phase of opening which consists of transmitting p data chosen between challenge phases to a decoder from a security element.
– The phase of the count which makes it possible to extract all or the part of scramble keys decrypted from p data chosen from the first n data into which it was put, and p data transmitted in the opening phase.
[0011] According to the specific embodiment of this invention, the method of transmitting the decrypted scramble key is as follows.
– Each first n data into which it was put is as a result of the first exclusive–OR function applied to the first data and 2nd data, the first data are pseudo–random WORD generated from adding seed to the first pseudo–random generation machine, and the 2nd data is WORD generated from being connected with all of the 3rd data and the decrypted scramble keys, or a part.
[0012] – An opening phase consists of transmitting seed and the 2nd data to a decoder from a security element.
– The phase of count consists of a degree.
– Calculate the 4th data based on applying seed to the 2nd pseudo–random generation machine.
[0013] – In order to calculate the 5th data, apply the 4th data and guaranteed data to the 2nd exclusive–OR function.
– Compare the 5th data with the 2nd data transmitted between actuation of opening.
– If it turns out that it is the same as that of the 2nd data with which the 5th data was transmitted between actuation of opening as a result of a comparison, store decrypted all or the part of scramble keys.
[0014] The advantage of this invention is protecting an exchange of the data between a security element and a decoder.
[0015]
[Embodiment of the Invention] Other descriptions and advantages of this invention become clear by reading one desirable embodiment of this invention with reference to an accompanying drawing. In the accompanying drawing, the same sign shows the same element. Drawing 1 shows fundamental drawing of the approach of transmitting the scramble key decrypted between the security element 1 and the decoder 2. A security element is a smart card preferably.
[0016] As mentioned above, a scramble key is transmitted to a decoder 2 from a smart card 1 according to the principle of operation of putting in (pledge). The principle of operation which puts in data consists of putting into the 2nd side about a beginning side, without transmitting without encryption about the data defined

beforehand. Next, a beginning side shows the data which are not enciphered to the 2nd side between the continuing steps. It has possibility of checking the data of the side [2nd] which is not enciphered corresponding with the data into which it was put.
[0017] According to this invention, a beginning side is a smart card 1, the 2nd side is a decoder 2 and the data into which it is put consist of decrypted all or the part of scramble keys. The protocol for exchanging data between a smart card and a decoder consists of three phases intrinsically [the phase to put in (pledging), a challenge phase, and an opening phase].
[0018] In the phase to put in, the smart card 1 containing the decrypted scramble key exchanges a decoder 2 and a message. In the end of the phase to put in, a smart card 1 exchanges a decoder 2 and a message by the approach of having the item which consists of data which enable a decoder to attest the data showing all or the part of scramble keys which is the form of 1 to 1 and was decrypted, and a smart card. Vocabulary called the data which make it possible to attest a smart card should be understood to be what means the data which make it possible to check that the hack (disturbance) of the smart card is not carried out.
[0019] The information included in the decoder in the end of a guarantee phase as an advantageous point cannot obtain the data for attesting all of the decrypted scramble keys or a part, and a card in itself. In a challenge phase, in order to show which should be indicated among the data into which it was put, data are transmitted to a smart card from a decoder. It performs by the approach with random the data which should be indicated and into which it was put being shown preferably.
[0020] In an opening phase, a smart card transmits the data which should be indicated by the decoder. That is, the data for attesting all of the decrypted scramble keys or a part, and a smart card are transmitted. A smart card 1 consists of the set (X1, Y) of data, (X2, Y), ..., (Xn, Y).
[0021] Each data (Xj, Y) (j= 1, 2, ..., n) consists of data Y and data Xj. Data Y are decrypted all or the part of a scramble key. Data Xj are independent of a scramble key, and are data which make a smart card attest. Arrow heads M1, M2, ..., Mj, ..., Mn, C, O1, O2, ..., Op show the various exchanges between a smart card 1 and a decoder 2.
[0022] It is shown that arrow heads M1 and M2, ..., Mj, ..., Mn put in each data (X1, Y), (X2, Y), ..., (Xn, Y). Preferably, putting in Mj+1 of data (Xj+1, Y) is performed after putting in Mj of data (Xj, Y). According to the desirable embodiment of this invention, the phase to put in consists of three steps of M1, M2, and M3. More generally the phase to put in consists of an n step, and n is two or more integers.
[0023] The data (Xj, Y) into which it was put by the decoder 2 are expressed as Mj (Xj, Y). As an advantageous point, Data Mj (Xj, Y) cannot identify Data Xj and Y by itself as mentioned above. The arrow head C shows the challenge phase. In a challenge phase, the data d chosen at random preferably are transmitted to a smart card 1 from a decoder 2. According to an operation of Data d, the microprocessor of a smart card

1 transmits P data which chose p data and were chosen from n data (Z1, Y) contained in a smart card, (Z2, Y), ..., (Zj, Y), ..., (Zn, Y) in this way to a decoder 2 from a smart card 1.

[0024] Each data (Zj, Y) (j= 1, 2, ..., n) consists of data Y and data Zj. According to the embodiment of the beginning of this invention, Data Zj (j= 1, 2, ..., n) are the same as Data Xj, and the data (Zj, Y) of them are the same as data (Xj, Y).

[0025] According to other embodiments of this invention, Data Zj differ from Data Xj. According to the embodiment besides ******** of this invention, Data Zj are carrying out mutual relation with Data Xj. An expression called the mutual relation of Data Zj and Data Xj is applied to data (Zj, Y) and (Xj, Y) various circuits, and/or an operator, and makes the extract of Data Y, and coincidence attest a smart card. The example of such an embodiment is explained by drawing 2 .

[0026] n data (Z1, Y), (Z2, Y), ..., (Zj, Y), ..., p data chosen from (Zn, Y) consist of the set (Za1, Y) of data, (Za2, Y), ..., (Zap(s), Y). In the transfer to a decoder 2 from the smart card 1 of p data (Za1, Y), (Za2, Y), ..., (Zap, Y), arrow heads O1, O2, ..., Op express the opening of each data (Za1, Y), (Za2, Y), ..., (Zap, Y) in opening operation.

[0027] Each data (Za1, Y), (Za2, Y), ..., the data stored after the opening of (Zap, Y) at the decoder 2 are expressed as O1 (Za1, Y), O2 (Za2, Y), ..., Op (Zap, Y). Each p data Ok (Zak, Y) is in agreement with one of the data Mj (Xj, Y) into which it was put. An expression called the data Mj (Xj, Y) into which it was put, and the data Ok (Zak, Y) in agreement The data Ok (Zak, Y) whose data Zak correspond with Data Xj in the case of the embodiment of the beginning of this invention mentioned above, Or it should be understood that Data Zak mean Data Xj and the data Ok (Zak, Y) which are carrying out mutual relation in the case of other embodiments of this invention.

[0028] According to this invention, a decoder 2 extracts Data Y from the data Ok (Zak, Y) equivalent to Data Mj (Xj, Y) and Mj (Xj, Y), and consists of a means M0 which makes possible what a smart card 1 is attested for. Data Y are stored in memory circuit M when Data Y are extracted from Data Mj (Xj, Y) and Ok (Zak, Y) by the means M0.

[0029] According to the desirable embodiment of this invention, in an opening phase, the phase to put in relates to two data of (Za1, Y), and (Za2, Y) in relation to three data of (X1, Y), (X2, Y), and (X3, Y). Data Y are decrypted all or the part of scramble keys as mentioned above. When it is the part of the scramble key by which Data Y were decrypted, operation mentioned above is performed in each various parts which constitute a scramble key. If an example is given, each data Y which is the part of the decrypted scramble key will consist of 7 or 8 bits, and a scramble key will be thoroughly reconfigurated with ten pass. Each pass makes a circuit M0 extract Data Y. Perfect reconstruction of the enciphered scramble key KD is performed using memory circuit M.

[0030] According to this invention, as an advantageous point, the transfer to a decoder 2 from the smart card 1 of Data Y is performed to authentication and

coincidence of a smart card 1. Since the data which the smart card was not attested any longer, consequently were transmitted to the decoder must have been taken into consideration, it becomes impossible so, for the hacker who monitors the data exchanged between a smart card and a decoder to find out semantics to change these data.

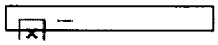
[0031] Drawing 2 expresses the specific embodiment of fundamental drawing shown in drawing 1 . Only putting in (pledging) and the operation of opening are expressed in drawing 2 . The various arrow heads from a smart card 1 to a decoder 2 express various exchanges of the data between a smart card 1 and a decoder 2.

[0032] The arrow head Mj means putting the data Cj contained in a smart card 1 into a decoder 2. Arrow heads Oa and Ob express the opening step equivalent to step Mj to put in. Since it is convenient, the exchange of the data between the smart cards 1 and decoders 2 which were expressed to drawing 2 relates to single step and single opening step. As mentioned above, according to the desirable embodiment of this invention, three data are put in by the decoder 2 and two opening steps (Oa, Ob) are actually performed from a smart card 1 to a decoder 2.

[0033] According to the specific embodiment of drawing 2 , a smart card 1 consists of the generation machine 3 of random WORD, the pseudo-random generation machine 4, an exclusive-OR function 5 6, for example, a data association circuit like a data connection circuit, and a separation operator 7, and a decoder 2 stores the pseudo-random generation machine 8, the exclusive-OR function 9, a comparison circuit 10, and the various data Y, and if required, it will consist of a circuit M which reconfigurates the perfect key KD from the various data Y.

[0034] The false data generation machine 8, the exclusive-OR function 9, and a comparison circuit 10 constitute the example of a circuit M0. The data Cj into which it was put are generated by applying Data Bj and Data Gj to the exclusive-OR function 5. So, [0035]

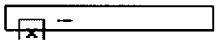
[Equation 1]



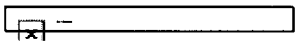
[0036] It can describe. Data Bj are pseudo-random WORD generated from the generation machine 4 with which Seed Sj is applied, and generate the seed Sj itself from the generation machine 3 of random WORD. Data Gj consist of WORD generated from association of Data Dj and Data Y. Association of Data Dj and Data Y is performed by connection.

[0037] According to the desirable embodiment of this invention, Data Y are the part of the decrypted scramble key KD which consists of b bits. As an example, b is equal to 7 or 8 bits respectively to the enciphered scramble key which consists of 70 or 80 bits. Data Y are generated from the separation circuit 7 where the decrypted scramble key KD is applied. The scramble key enciphered so that it might be well-known is transmitted to this contractor from a decoder 2 to a smart card 1, and a

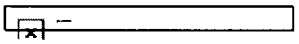
smart card 1 includes the decryption circuit (it has not indicated to drawing 2) which makes it possible to restore the decrypted key KD.
[0038] According to other embodiments of this invention, Data Y are the scramble key by which the whole was decrypted. According to this invention, an authentication procedure is activated whenever the enciphered scramble key is transmitted to a smart card 1 from a decoder 2. Since it is impossible to determine the data Bj generated from the pseudo-random generation machine 4, the expression with which 1 to 1 of the data Gj maintained at secrecy by Naka of Cj was enciphered is Data Cj.
[0039] If WORD Cj is transmitted to a decoder 2 from a smart card 1, the phase which Cj puts in will be completed. And an opening step is performed. In an opening step, two data Sj and Gj are transmitted to a decoder 2 from a smart card 1. Data Sj are transmitted by Opening Oa and Data Gj are transmitted by Opening Ob.
[0040] The transmitted seed Sj is applied to the pseudo-random generation machine 8. According to Seed's Sj operation, the pseudo-random generation machine 8 generates Data Ej. And the ** data Ej and Cj into which it was put are applied to the exclusive-OR function 9. The data Fj generated from the exclusive-OR function 9 are compared with Data Gj by the comparison circuit 10. If Data Ej are in agreement with Data Bj, Data Fj are in agreement with Data Gj.
[0041] It is here and is [0042].
[Equation 2]



[0043] Namely, [0044]
[Equation 3]



[0045] It will be [0046] if it becomes Ej=Bj.
[Equation 4]



[0047] namely, Fj=Gj -- so, the comparison operator 10 checks whether Data Fj are the same as Data Gj, or it is not the same. In such a case, Data Y are stored in Memory M. The scramble key by which the transfer of the scramble key from the smart card 1 using Challenge Handshake Authentication Protocol which was explained by drawing 1 and drawing 2 as an advantageous point to a decoder 2, on the other hand, corroborated that it was not the card with which a smart card is an authentication card and was hacked, and was transmitted to the decoder 2 on the other hand corroborates being taken out from the smart card which is not hacked truly.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] Fundamental drawing of the approach of transmitting the scramble key decrypted between the security element and the decoder by this invention is shown.

[Drawing 2] The specific embodiment of a step with the approach shown in drawing 1 is shown.

[Description of Notations]

1 Security Element

2 Decoder

3 Generation Machine of Random WORD

4 Pseudo-random Generation Machine

5 Exclusive-OR Function

6 Data Association Circuit

7 Separation Operator

8 Pseudo-random Generation Machine

9 Exclusive-OR Function

10 Comparison Circuit

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－196083

(43)公開日　平成11年(1999)７月21日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ｂ
9/32			６７５Ａ

審査請求　未請求　請求項の数５　ＯＬ　（全７頁）

(21)出願番号　特願平10－293845

(22)出願日　平成10年(1998)10月15日

(31)優先権主張番号　９７１３０２２

(32)優先日　1997年10月17日

(33)優先権主張国　フランス（ＦＲ）

(71)出願人　391000771
トムソン　マルチメデイア　ソシエテ　アノニム
THOMSON MULTIMEDIA S. A.
フランス国, 92648　ブローニュ　セデックス, ケ・アルフォンス・ル・ガロ　46

(72)発明者　アルナルド　カンピノ
フランス国, 75017　パリ, リュ・ド・ソシュル　36－38

(72)発明者　ジャンーベルナール　フィッシェール
フランス国, 94270　ル・クレムラン・ビセートル, リュ・カルノ　38

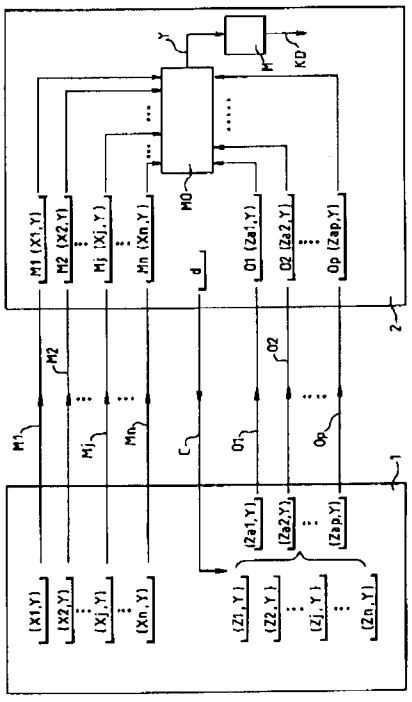
(74)代理人　弁理士　伊東　忠彦　（外１名）

(54)【発明の名称】　スクランブルキー転送方法

(57)【要約】

【課題】本発明はセキュリティーエレメントからデコーダへスクランブルキーを転送する方法に関する。

【解決手段】転送方法は、入れる段階、チャレンジ段階及びオープニング段階からなる。入れる段階では、暗号解読されたスクランブルキーを含むセキュリティーエレメントはデコーダとメッセージを交換し、その結果、入れる段階の終わりにおいて、デコーダは、１対１の形で、暗号解読されたスクランブルキーの全部または部分を表すデータ及びスマートカードを認証することを可能とするデータを表すデータからなる項目を有し、チャレンジ段階では、データはデコーダからスマートカードに転送され、その結果、入れられたデータのうちのどれが開示されるかを表す。好ましくは、開示される入れられるデータの明示はランダムに行われる。オープニング段階では、スマートカードは、開示されるべきデータ、すなわち、スマートカードを認証することを可能とするデータとともに、暗号解読されたスクランブルキーの全部または部分であるデータをデコーダに転送する。



【特許請求の範囲】
【請求項1 】セキュリティーエレメント（１）からデコーダ（２）へ暗号解読されたスクランブルキーを転送する方法において、
セキュリティーエレメント（１）から出力されたｎ個の最初のデータ（（Ｘ１、Ｙ）、（Ｘ２、Ｙ）、・・・、（Ｘｎ、Ｙ））をデコーダ（２）の中に入れる（Ｍ１、Ｍ２、・・・、Ｍｊ、・・・、Ｍｎ）段階であって、前記ｎは２以上の整数であり、前記ｎ個の最初に入れられた各データは暗号解読されたスクランブルキー（ＫＤ）の全てまたは部分（Ｙ）及びセキュリティーエレメント（１）を認証させる最初のデータ（Ｘｊ）からなる段階と、
ｎ個の第２のデータ（（Ｚ１、Ｙ）、（Ｚ２、Ｙ）、・・・、（Ｚｊ、Ｙ）、・・・、（Ｚｎ、Ｙ））からｐ個のデータ（（Ｚａ１、Ｙ）、（Ｚａ２、Ｙ）、・・・、（Ｚａｐ、Ｙ））を選択することを可能とするデータ（ｄ）がデコーダ（２）からセキュリティーエレメント（１）へ転送されるチャレンジ（Ｃ）の段階であって、前記ｐはｎより小さい整数であり、前記ｎ個の第２の各データは、暗号解読されたスクランブルキーの全部または部分（Ｙ）及びセキュリティーエレメント（１）の認証をさせる第２のデータ（Ｘｊ）からなる段階と、
セキュリティーエレメント（１）からデコーダ（２）に、チャレンジ段階（Ｃ）で選択されたｐ個のデータの転送からなるオープニング（Ｏ１、Ｏ２、・・・、Ｏｐ）の段階と、
ｎ個の最初の入れられたデータ（（Ｘ１、Ｙ）、（Ｘ２、Ｙ）、・・・、（Ｘｎ、Ｙ））から選択されたｐ個のデータ及びオープニング段階にて転送されたｐ個のデータ（Ｏ１（Ｚａ１、Ｙ）、Ｏ２（Ｚａ２、Ｙ）、・・・、Ｏｐ（Ｚａｐ、Ｙ））から暗号解読されたスクランブルキーの全てまたは部分（Ｙ）を抽出することを可能とする計算段階とからなることを特徴とする方法。
【請求項２】前記計算段階の後、前記入れる段階、オープニング段階及び計算段階が完全なスクランブルキー（ＫＤ）の一部分（Ｙ）に関連する場合に、完全なスクランブルキーを再構築する段階からなる請求項１記載の方法。
【請求項３】前記入れる段階（Ｍ１、Ｍ２、・・・、Ｍｊ、・・・、Ｍｎ）は３ステップ（Ｍ１、Ｍ２、Ｍ３）からなり、オープニングステップ（Ｏ１、Ｏ２、・・・、Ｏｐ）は２ステップからなる請求項１または２に記載の方法。
【請求項４】ｐ個のデータ（（Ｚａ１、Ｙ）、（Ｚａ２、Ｙ）、・・・、（Ｚａｐ、Ｙ））をｎ個の第２のデータ（（Ｚ１、Ｙ）、（Ｚ２、Ｙ）、・・・、（Ｚｊ、Ｙ）、・・・、（Ｚｎ、Ｙ））から選択することはランダムに行われる請求項１ないし３のうちいずれか１項に記載の方法。
【請求項５】ｎ個の最初に入れられたデータの各々（Ｃｊ）は、最初のデータ（Ｂｊ）及び第２のデータ（Ｇｊ）が適用される最初の排他的論理和機能（５）の結果であり、前記最初のデータ（Ｂｊ）は、シード（Ｓｊ）を最初の擬似ランダム生成器（４）に適用して発生する擬似ランダムワードであり、前記第２のデータ（Ｇｊ）は、第３のデータおよび暗号解読されたスクランブルキー（Ｙ）の全部または部分を関連させることから発生するワードであり、
前記オープニング段階はセキュリティーエレメント（１）からデコーダ（２）に、シード（Ｓｊ）及び第２のデータ（Ｇｊ）を転送することからなり、
前記計算段階は、
シードＳｊを第２の擬似ランダム生成器（８）に適用することによる第４のデータ（Ｅｊ）を計算し、
第５のデータ（Ｆｊ）を計算するために、第４のデータ（Ｅｊ）及び入れられたデータ（Ｃｊ）を第２の排他的論理和機能（９）に適用し、
第５のデータ（Ｆｊ）をオープニングオペレーションにて転送される第２のデータ（Ｇｊ）と比較し、
比較の結果、第５のデータ（Ｆｊ）がオープニングオペレーションにて転送される第２のデータ（Ｇｊ）と同一であれば、暗号解読されたスクランブルキーの全部または部分（Ｙ）を格納することからなる請求項１ないし４のうちいずれか１項記載の方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明はスクランブルキーを転送する方法に関し、特に、条件付きアクセスシステムのセキュリティーエレメントとデコーダの間でスクランブルキーを転送する方法に関する。条件付きアクセスシステムによりサービスプロバイダは自分のサービスをそのサービスを受ける権利を獲得したユーザだけに提供することができる。このようなシステムには、例えば、有料テレビジョンシステムがある。
【０００２】
【従来の技術】当業者に公知の如く、サービスプロバイダによって提供されたサービスは、スクランブルキーによりスクランブルをかけられた項目からなる。スクランブルをかけられた項目は、ユーザに割り当てられた権利のレベルで、スクランブルを解除せられ、ユーザに読まれる。スクランブルされた項目は以下ＩＥ（ＥＣＧ）と表記される。ＥＣＧはスクランブルされていない項目を表す（ＥＣＧは"Electronically Coded Goods"の略である）。
【０００３】項目をスクランブル解除するため、サービスプロバイダは、項目をスクランブルするために用いられるスクランブルキーを各ユーザに供給する。スクランブルキーを秘密に保つため、スクランブルキーはキーＫを用いたアルゴリズムで暗号化された後に供給される。

種々の暗号化されたスクランブルキーは制御メッセージにおいて種々のユーザに送られる。以下、制御メッセージはＥＣＭと表記される（ＥＣＭは"Entitlement Control Message"の略である）。

【０００４】権利を与えられたユーザにだけサービスへのアクセスを与えるために、サービスプロバイダは各ユーザにスマートカードとデコーダを提供する。ＥＣＭはデコーダにより受信され、デコーダはそれらをスマートカードに転送する。スマートカードはスクランブルキーの暗号化アルゴリズムのキーＫを含む。スクランブルキーはスマートカードにより解読され、デコーダにリストアされ、デコーダは受信したスクランブルされた項目のスクランブル解除をすることができる。

【０００５】

【発明が解決しようとする課題】スマートカードとデコーダの間をモニタするハッカーは、スマートカードからデコーダへ流れる暗号解読されたスクランブルキーを傍受する位置にいる。これが欠点を表すものである。条件付きアクセスシステムはスタンドアロンタイプのシステムであり、そのシステムではスクランブルされた項目ＩＥ（ＥＣＧ）及びＥＣＭが、例えばデジタルビデオディスクのようなスタンドアロンの情報キャリア上に含まれているため、この欠点はさらに重大なものである。なぜならば、暗号化されていないスクランブルキーを傍受するハッカーはこれらのキーをストアでき、不正に、許可を受けていないユーザのそれらを再配布することができるからである。スタンドアロン情報キャリア上に含まれるスクランブルされた項目はもはや保護されていないことになる。

【０００６】条件付きアクセスシステムがオンラインタイプである場合、スクランブルされた項目ＩＥ（ＥＣＧ）は、空間またはケーブル上を単一の源からサービスプロバイダの種々の顧客へ同時に配布された信号から構成される項目である。解読されたスクランブルキーはリアルタイムでハック（侵害）されなければならない。ハッキングの条件はより難しくなる。しかしながら、ハッキングの危険性は十分に短いリンク上では比較的高いままである。

【０００７】本発明にはこれらの欠点がない。

【０００８】

【課題を解決するための手段】本発明は、セキュリティーエレメントからデコーダへ暗号解読されたスクランブルキーを転送する方法に関する。上記転送する方法は次の段階からなる。

ーデコーダにおいて、セキュリティーエレメントからの最初のｎ個のデータ出力を入れる（ｐｌｅｄｇｅ）段階であり、ｎは２以上の整数、最初のｎ個の入れられた各データは、暗号解読されたスクランブルキーの全部または部分、及び、セキュリティーエレメントの認証をさせる最初のデータからなる。

【０００９】ー第２のｎ個のデータからｐ個のデータを選択することを可能とする１個のデータがデコーダからセキュリティーエレメントへ転送されるチャレンジの段階であり、ｐはｎより小さい整数であり、第２のｎ個の各データは、暗号解読されたスクランブルキーの全部または部分、及び、セキュリティーエレメントの認証をさせる第２のデータからなる。

【００１０】ーチャレンジ段階の間に選択されたｐ個のデータをセキュリティーエレメントからデコーダに転送することからなるオープニングの段階。

ー最初のｎ個の入れられたデータから選択されたｐ個のデータ、及び、オープニング段階で転送されたｐ個のデータから暗号解読されたスクランブルキーの全部または部分を抽出することを可能とする計算の段階。

【００１１】本発明の特定の実施態様によれば、暗号解読されたスクランブルキーを転送する方法は次の通りである。

ー最初のｎ個の入れられた各データは、最初のデータ及び第２のデータに適用される最初の排他的論理和機能の結果であり、最初のデータは、最初の擬似ランダム生成器へシードを加えることから発生する擬似ランダムワードであり、第２のデータは第３のデータ、及び、暗号解読されたスクランブルキーの全部または部分と関連することから発生するワードである。

【００１２】ーオープニング段階は、シード及び第２のデータを、セキュリティーエレメントからデコーダへ転送することからなる。

ー計算の段階は次からなる。

ーシードを第２の擬似ランダム生成器に適用することによる第４のデータを計算すること。

【００１３】ー第５のデータを計算するために、第４のデータ及び保証されたデータを、第２の排他的論理和機能に適用すること。

ー第５のデータを、オープニングの動作の間に転送された第２のデータと比較すること。

ー比較の結果、第５のデータがオープニングの動作の間に転送された第２のデータと同一であることがわかれば、暗号解読されたスクランブルキーの全部または部分を格納すること。

【００１４】本発明の利点は、セキュリティーエレメントとデコーダ間のデータのやりとりを保護することである。

【００１５】

【発明の実施の形態】本発明の他の特徴及び利点は、添付図面を参照して本発明の好ましい一実施態様を読むことにより明らかになる。添付図面において、同じ符号は同じ要素を示している。図１は、セキュリティーエレメント１とデコーダ２の間で暗号解読されたスクランブルキーを転送する方法の基本的な図を示している。セキュリティーエレメントは好ましくはスマートカードであ

る。

【００１６】前述したように、スクランブルキーは、入れること（ｐｌｅｄｇｅ）の動作原理に従いスマートカード１からデコーダ２へ転送される。データを入れる動作原理は、最初の側については、予め定められたデータに関して、暗号化なしで転送することなく、第２の側に入れることからなる。次に続くステップの間、最初の側は暗号化されていないデータを第２の側に示す。第２の側は、その暗号化されていないデータが、入れられたデータと一致することを確認する可能性を有する。

【００１７】本発明によれば、最初の側はスマートカード１であり、第２の側はデコーダ２であり、入れられるデータは暗号解読されたスクランブルキーの全部または部分からなる。スマートカードとデコーダの間でデータを交換するためのプロトコルは、入れる（ｐｌｅｄｇｉｎｇ）段階、チャレンジ段階、オープニング段階の本質的に３つの段階からなる。

【００１８】入れる段階において、暗号解読されたスクランブルキーを含むスマートカード１は、デコーダ２とメッセージを交換する。入れる段階の終わりにおいて、デコーダは、１対１の形で、暗号解読されたスクランブルキーの全部または部分を表すデータとスマートカードを認証することを可能とするデータからなる項目を有する、という方法でスマートカード１は、デコーダ２とメッセージを交換する。スマートカードを認証することを可能とするデータという用語はスマートカードがハック（侵害）されていないことを確認することを可能とするデータを意味するものと理解されるべきである。

【００１９】有利な点として、保証段階の終わりにおけるデコーダに含まれる情報は、それ自身では暗号解読されたスクランブルキーの全部または部分、及びカードを認証するためのデータを得ることはできない。チャレンジ段階において、入れられたデータのうちどれが開示されるべきかを示すために、データがデコーダからスマートカードに転送される。好ましくは、開示されるべき入れられたデータを示すことは、ランダムな方法で実行される。

【００２０】オープニング段階において、スマートカードはデコーダに開示されるべきデータを転送する。すなわち、暗号解読されたスクランブルキーの全部または部分、及びスマートカードを認証するためのデータを転送する。スマートカード１はデータのセット（Ｘ１、Ｙ）、（Ｘ２、Ｙ）、・・・、（Ｘｎ、Ｙ）からなる。

【００２１】各データ（Ｘｊ、Ｙ）（ｊ＝１、２、・・・、ｎ）は、データＹとデータＸｊからなる。データＹは暗号解読されたスクランブルキーの全てまたは部分である。データＸｊはスクランブルキーとは独立で、スマートカードの認証をさせるデータである。矢印Ｍ１、Ｍ２、・・・、Ｍｊ、・・・、Ｍｎ、Ｃ、Ｏ１、Ｏ２、・・・、Ｏｐはスマートカード１とデコーダ２の間の種々のやりとりを示している。

【００２２】矢印Ｍ１、Ｍ２、・・・、Ｍｊ、・・・、Ｍｎは各データ（Ｘ１、Ｙ）、（Ｘ２、Ｙ）、・・・、（Ｘｎ、Ｙ）を入れることを示している。好ましくは、データ（Ｘｊ＋１、Ｙ）のＭｊ＋１を入れることは、データ（Ｘｊ、Ｙ）のＭｊを入れることに続いて行われる。本発明の好ましい実施態様によれば、入れる段階はＭ１、Ｍ２、Ｍ３の３ステップからなる。より一般的には、入れる段階はｎステップからなり、ｎは２以上の整数である。

【００２３】デコーダ２に入れられたデータ（Ｘｊ、Ｙ）はＭｊ（Ｘｊ、Ｙ）と表される。有利な点として、前述した通り、データＭｊ（Ｘｊ、Ｙ）は、それ自身ではデータＸｊとＹを識別できない。矢印Ｃはチャレンジ段階を示している。チャレンジ段階において、好ましくはランダムに選択されるデータｄはデコーダ２からスマートカード１に転送される。データｄの作用により、スマートカード１のマイクロプロセッサはスマートカードに含まれるｎ個のデータ（Ｚ１、Ｙ）、（Ｚ２、Ｙ）、・・・、（Ｚｊ、Ｙ）、・・・、（Ｚｎ、Ｙ）からｐ個のデータを選択し、このように選択されたＰ個のデータをスマートカード１からデコーダ２に転送する。

【００２４】各データ（Ｚｊ、Ｙ）（ｊ＝１、２、・・・、ｎ）はデータＹ及びデータＺｊからなる。本発明の最初の実施態様によれば、データＺｊ（ｊ＝１、２、・・・、ｎ）はデータＸｊと同一であり、データ（Ｚｊ、Ｙ）はデータ（Ｘｊ、Ｙ）と同一である。

【００２５】本発明の他の実施態様によれば、データＺｊはデータＸｊと異なる。本発明ののこれら他の実施態様によれば、しかしながら、データＺｊはデータＸｊと相互関連している。データＺｊとデータＸｊの相互関連という表現は、データ（Ｚｊ、Ｙ）及び（Ｘｊ、Ｙ）は、種々の回路及び／またはオペレータに適用され、データＹの抽出、及び、同時にスマートカードの認証をさせる。このような実施態様の例は図２で説明される。

【００２６】ｎ個のデータ（Ｚ１、Ｙ）、（Ｚ２、Ｙ）、・・・、（Ｚｊ、Ｙ）、・・・、（Ｚｎ、Ｙ）から選択されるｐ個のデータはデータのセット（Ｚａ１、Ｙ）、（Ｚａ２、Ｙ）、・・・、（Ｚａｐ、Ｙ）からなる。ｐ個のデータ（Ｚａ１、Ｙ）、（Ｚａ２、Ｙ）、・・・、（Ｚａｐ、Ｙ）のスマートカード１からデコーダ２への転送は、オープニングオペレーションに当たり、矢印Ｏ１、Ｏ２、・・・、Ｏｐはそれぞれのデータ（Ｚａ１、Ｙ）、（Ｚａ２、Ｙ）、・・・、（Ｚａｐ、Ｙ）のオープニングを表す。

【００２７】それぞれのデータ（Ｚａ１、Ｙ）、（Ｚａ２、Ｙ）、・・・、（Ｚａｐ、Ｙ）のオープニングの後にデコーダ２に格納されたデータはＯ１（Ｚａ１、Ｙ）、Ｏ２（Ｚａ２、Ｙ）、・・・、Ｏｐ（Ｚａｐ、Ｙ）と表される。ｐ個の各データＯｋ（Ｚａｋ、Ｙ）は

入れられたデータＭｊ（Ｘｊ、Ｙ）の一つと一致する。入れられたデータＭｊ（Ｘｊ、Ｙ）と一致するデータＯｋ（Ｚａｋ、Ｙ）という表現は、上述した本発明の最初の実施態様の場合において、データＺａｋがデータＸｊと一致しているデータＯｋ（Ｚａｋ、Ｙ）、または、本発明の他の実施態様の場合において、データＺａｋがデータＸｊと相互関連しているデータＯｋ（Ｚａｋ、Ｙ）を意味すると理解されるべきである。

【００２８】本発明によれば、デコーダ２は、データＭｊ（Ｘｊ、Ｙ）及びＭｊ（Ｘｊ、Ｙ）に相当するデータＯｋ（Ｚａｋ、Ｙ）からデータＹを抽出し、スマートカード１を認証する、ことを可能とする手段Ｍ０からなる。手段Ｍ０によりデータＹがデータＭｊ（Ｘｊ、Ｙ）及びＯｋ（Ｚａｋ、Ｙ）から抽出されると、データＹはメモリ回路Ｍに格納される。

【００２９】本発明の好ましい実施態様によれば、入れる段階は（Ｘ１、Ｙ）、（Ｘ２、Ｙ）、（Ｘ３、Ｙ）の３データに関連し、オープニング段階は（Ｚａ１、Ｙ）、（Ｚａ２、Ｙ）の２データに関連する。前述した通り、データＹは暗号解読されたスクランブルキーの全部または部分である。データＹが暗号解読されたスクランブルキーの部分である場合、上述した入れるオペレーションはスクランブルキーを構成する種々の各部分で実行される。例を挙げると、暗号解読されたスクランブルキーの部分である各データＹは７または８ビットからなり、スクランブルキーは１０パスで完全に再構成される。各パスは回路Ｍ０によりデータＹの抽出をさせる。暗号化されたスクランブルキーＫＤの完全な再構成はメモリ回路Ｍを用いて実行される。

【００３０】有利な点として、本発明によれば、データＹのスマートカード１からデコーダ２への転送は、スマートカード１の認証と同時に行われる。それゆえ、スマートカードはもはや認証されず、その結果、デコーダに転送されたデータは考慮され得ないので、スマートカードとデコーダの間でやりとりされるデータを傍受するハッカーは、これらのデータを変更することに意味を見出せなくなる。

【００３１】図２は、図１に示された基本的な図の特定の実施態様を表す。図２においては、入れること（ｐｌｅｄｇｉｎｇ）とオープニングのオペレーションのみが表されている。スマートカード１からデコーダ２への種々の矢印は、スマートカード１とデコーダ２の間のデータの種々のやりとりを表している。

【００３２】矢印Ｍｊは、スマートカード１に含まれるデータＣｊをデコーダ２に入れることを表している。矢印Ｏａ及びＯｂは入れるステップＭｊに相当するオープニングステップを表している。便利のため、図２に表されたスマートカード１とデコーダ２の間のデータのやりとりは、単一の入れるステップ及び単一のオープニングステップに関連している。実際、前述したように、本発明の好ましい実施態様によれば、３データはデコーダ２に入れられ、２つのオープニングステップ（Ｏａ、Ｏｂ）がスマートカード１からデコーダ２に対して実行される。

【００３３】図２の特定の実施態様によれば、スマートカード１はランダムワードの生成器３、擬似ランダム生成器４、排他的論理和機能５、例えばデータ連結回路のようなデータアソシエーション回路６、分離オペレータ７からなり、デコーダ２は、擬似ランダム生成器８、排他的論理和機能９、比較回路１０、及び、種々のデータＹを格納し、必要ならば種々のデータＹから完全なキーＫＤを再構成する回路Ｍからなる。

【００３４】擬似データ生成器８、排他的論理和機能９及び比較回路１０は回路Ｍ０の例を構成する。入れられたデータＣｊは、データＢｊとデータＧｊを排他的論理和機能５に適用することにより発生する。それゆえ、

【００３５】

【数１】

$$Cj = Bj \oplus Gj$$

【００３６】と記述し得る。データＢｊはシードＳｊが適用される生成器４から発生する擬似ランダムワードであり、シードＳｊ自身はランダムワードの生成器３から発生する。データＧｊは、データＤｊとデータＹの結合から発生するワードからなる。データＤｊとデータＹの結合は例えば連結により実行される。

【００３７】本発明の好ましい実施態様によれば、データＹはｂビットからなる暗号解読されたスクランブルキーＫＤの部分である。例として、ｂは、７０または８０ビットからなる暗号化されたスクランブルキーに対してそれぞれ７または８ビットに等しい。データＹは、暗号解読されたスクランブルキーＫＤが適用される分離回路７から発生する。当業者には公知の如く、暗号化されたスクランブルキーはデコーダ２からスマートカード１へ転送され、スマートカード１は暗号解読されたキーＫＤをリストアすることを可能とする暗号解読回路（図２には記載していない）を含む。

【００３８】本発明の他の実施態様によれば、データＹは全体の暗号解読されたスクランブルキーである。本発明によれば、認証手順は、暗号化されたスクランブルキーがデコーダ２からスマートカード１へ転送される度に活性化される。擬似ランダム生成器４から発生するデータＢｊを決定することは不可能であるため、Ｃｊの中で秘密に保たれるデータＧｊの１対１の暗号化された表現はデータＣｊである。

【００３９】ワードＣｊをスマートカード１からデコーダ２へ転送すると、Ｃｊの入れる段階は完了する。そして、オープニングステップが実行される。オープニングステップにおいて、２個のデータＳｊとＧｊがスマートカード１からデコーダ２に転送される。データＳｊはオープニングＯａにより転送され、データＧｊはオープニ

ングＯｂにより転送される。

【００４０】転送されたシードＳｊは擬似ランダム生成器８に適用される。シードＳｊの作用により、擬似ランダム生成器８はデータＥｊを生成する。そして、入れられたたデータＥｊとＣｊは排他的論理和機能９に適用される。排他的論理和機能９から生成するデータＦｊは、比較回路１０によりデータＧｊと比較される。データＥｊがデータＢｊと一致すれば、データＦｊはデータＧｊに一致する。

【００４１】ここで

【００４２】

【数２】

$$Fj = Ej \oplus Cj$$

【００４３】すなわち

【００４４】

【数３】

$$Fj = Ej \oplus Bj \oplus Gj$$

【００４５】もし、Ｅｊ＝Ｂｊならば、

【００４６】

【数４】

$$Fj = Bj \oplus Bj \oplus Gj$$

【００４７】すなわち、Ｆｊ＝Ｇｊ

それゆえ、比較オペレータ１０は、データＦｊがデータＧｊと同一か同一でないかを確認する。そのような場合は、データＹはメモリＭに格納される。有利な点として、図１及び図２で説明したような認証プロトコルを用いたスマートカード１からデコーダ２へのスクランブルキーの転送は、一方ではスマートカードが認証カードでありハッキングされたカードでないことを確証し、他方ではデコーダ２に転送されたスクランブルキーが本当にハッキングされていないスマートカードから出されたものであることを確証する。

【図面の簡単な説明】

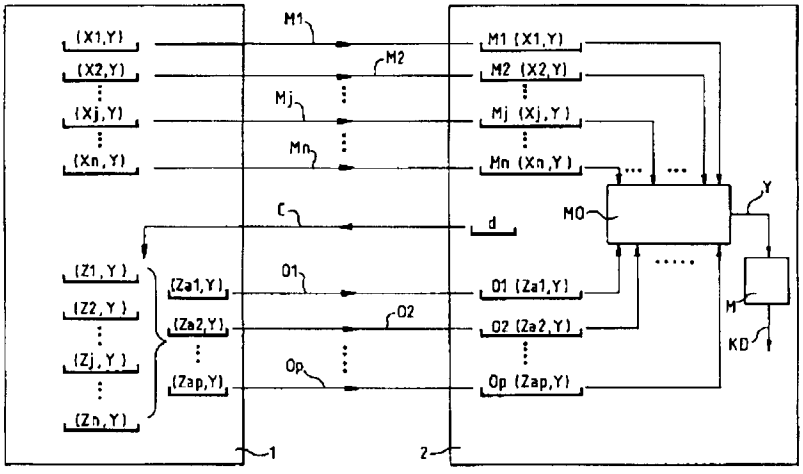
【図１】本発明により、セキュリティーエレメントとデコーダの間で暗号解読されたスクランブルキーを転送する方法の基本的な図を示している。

【図２】図１に示す方法のあるステップの特定の実施態様を示す。

【符号の説明】

１　セキュリティーエレメント
２　デコーダ
３　ランダムワードの生成器
４　擬似ランダム生成器
５　排他的論理和機能
６　データアソシエーション回路
７　分離オペレータ
８　擬似ランダム生成器
９　排他的論理和機能
１０　比較回路

【図１】



【図２】